JOURNAL OF ALGEBRA **184,** 881–896 (1996)
ARTICLE NO. 0289

Minimal Noncryptic e-Varieties of Regular Semigroups

F. Pastijn

Department of Mathematics, Statistics and Computer Science, Marquette University, Milwaukee, Wisconsin 53233

and

M. V. Volkov

Department of Mathematics and Mechanics, Ural State University, 620083 Ekatherinburg, Russia

Communicated by T. E. Hall

Received February 15, 1995

We describe all minimal noncryptic e-varieties of regular semigroups, thus generalising earlier results by Rasin and Reilly that dealt with the completely regular and the inverse cases, respectively. As corollaries, we prove that an e-variety of regular semigroups is cryptic if and only if its intersections with the variety of all completely regular semigroups and the variety of all inverse semigroups are cryptic. We also find an equational characterization of group-bound cryptic varieties; this generalises some recent results by Doyle and Yeh.

INTRODUCTION AND SUMMARY

Recall that a regular semigroup S is called *cryptic* if Green's relation $\mathscr{H}$ happens to be a congruence on S and a variety is said to be cryptic if each of its members is a cryptic semigroup. A noncryptic variety $\mathscr{V}$ is called *minimal noncryptic* if all its proper subvarieties are cryptic.

Cryptic and minimal noncryptic varieties have been intensively studied in various classes of regular semigroups. For a complete regular semigroup, being cryptic means exactly being a band of groups, and the importance of the class of varieties of bands of groups is very well known

0021-8693/96 $18.00

(see, e.g., [5, 7]). In particular, in the latter paper all the minimal noncryptic varieties of completely regular semigroups were described. Let us formulate the corresponding result.

For each prime number p, consider semigroups

$$L(p) = \langle e, g | eg = e = e^2 = g^p e,\ g^{p+1} = g \rangle$$

and

$$R(p) = \langle e, g | ge = e = e^2 = eg^p,\ g^{p+1} = g \rangle.$$

THEOREM 1 (Rasin [7]). *A completely regular semigroup variety is minimal noncryptic if and only if it is generated by exactly one of the semigroups $L(p)$ or $R(p)$ for some prime p and every noncryptic variety of completely regular semigroups contains a minimal noncryptic one.*

Another class of regular semigroups in which cryptic and minimal noncryptic varieties have been investigated is the class of inverse semigroups (see [8, 9]). Again the second of these papers contains a nice description of minimal noncryptic inverse semigroup varieties. To formulate it, we need a construction from [9].

For each group G, consider the Brandt semigroup $M(G, E, G, \Delta)$ over the one-element group $E = \{e\}$ and define a multiplication on the disjoint union $N(G, G)$ of G and $M(G, E, G, \Delta)$ by preserving the multiplications on G and $M(G, E, G, \Delta)$ and letting, for all $g \in G$, $[h, e, k] \in M(G, E, G, \Delta)$,

$$g[h, e, k] = [hg^{-1}, e, k], \qquad [h, e, k]g = [h, e, kg], \qquad g0 = 0g = 0.$$

Then $N(G, G)$ becomes an inverse semigroup.

Denote by $\mathbf{C}_\infty$ (resp., $\mathbf{C}_p$) the infinite cyclic group (resp., the cyclic group of the prime order p).

THEOREM 2 (Reilly [9, Corollary 6.4]). *An inverse semigroup variety is minimal noncryptic if and only if it is generated by exactly one of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ or $N(\mathbf{C}_p, \mathbf{C}_p)$ for some prime p and every noncryptic variety of inverse semigroups contains a minimal noncryptic one.*

Recall that class $\mathscr{V}$ of regular semigroups is said to be an *existence variety* (or *e-variety*) if it is closed under taking direct products, regular subsemigroups, and homomorphic images. Since this notion was introduced by Hall [3] (and, independently, by Kaďourek and Szendrei [6] for the class of orthodox semigroups), several authors have expanded some of the results about cryptic varieties of inverse and completely regular semigroups to larger classes of regular semigroups. Thus, Doyle has characterized cryptic e-varieties of orthodox semigroups and proved, in particular, that an e-variety of orthodox semigroups is cryptic if and only if its intersections with the variety of all completely regular semigroups and the variety of all inverse semigroups are cryptic [2, Theorem 4.7]. Yeh [10] considered cryptic e-varieties of E-solid semigroups. (Recall that a semigroup S is called *E-solid* if for all idempotents $e, f, g \in S$ such that $e\mathscr{L}f\mathscr{R}g$, there exists an idempotent $h \in S$ such that $e\mathscr{R}h\mathscr{L}g$.)

The aim of the present paper is to describe all minimal-noncryptic e-varieties of regular semigroups. We prove the following (slightly surprising) result.

THEOREM 3. *An e-variety of regular semigroups is minimal noncryptic if and only if it is generated by exactly one of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$, $N(\mathbf{C}_p, \mathbf{C}_p)$, $L(p)$, or $R(p)$ for some prime p and every noncryptic e-variety of regular semigroups contains a minimal noncryptic one.*

Theorem 3 is proved in Section 2, whereas Section 1 is devoted to studying a construction generalising simultaneously those of [7] and [9]. Section 3 contains some corollaries and applications of the main result. One of them seems to deserve being formulated here for it is of independent interest. We call a semigroup S *group-closed* if the union $\operatorname{Gr} S$ of all its subgroups is a subsemigroup in S. The notions of a *group-closed* e-variety and a *minimal non-group-closed* e-variety are defined in the usual way. Let C_2 denote the five-element idempotent generated 0-simple semigroup that can be represented as a Rees matrix semigroup over the one-element group $E = \{e\}$ with the sandwich matrix $\left[\begin{smallmatrix} e & e \\ 0 & e \end{smallmatrix}\right]$.

THEOREM 4. *An e-variety of regular semigroups is minimal non-group-closed if and only if it is generated by exactly one of the semigroups C_2, $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ or $N(\mathbf{C}_p, \mathbf{C}_p)$ for some prime p and every non-group-closed e-variety of regular semigroups contains a minimal non-group-closed one.*

Theorems 3 and 4 lead to an interesting interplay between the properties "being cryptic" and "being group-closed," which is analyzed in Section 3.

1. A CONSTRUCTION

Let G be a group and L, R be subgroups of G. Denote by G_L (${}_RG$) the collection of all left (resp., right) cosets of G with respect to L (resp., R) and by ${}_RG_L$ the collection of all *double cosets* with respect to the semigroups R and L, i.e., all subsets of the kind RgL, where g runs over G.

Let A be any subset of ${}_RG_L$ containing RL. Consider the Rees matrix semigroups $M(G_L, E, {}_RG, P_A)$ over the one-element semigroup $E = \{e\}$, where $P_A = (p_{Rk,hL})$ is a ${}_RG \times G_L$ matrix defined by the rule

$$p_{Rk,hL} = \begin{cases} e, & \text{if } RkhL \in A, \\ 0, & \text{otherwise}. \end{cases}$$

For $hL \in G_L$, $Rk \in {}_RG$, we denote the element $[hL, e, Rk]$ of the semigroup $M(G_L, E, {}_RG, P_A)$ simply by $[hL, Rk]$.

Now let $T(G, L, R, A)$ denote the disjoint union of the group G and the semigroup $M(G_L, E, {}_RG, P_A)$. We define a multiplication on this union by extending the multiplication on both G and $M(G_L, E, {}_RG, P_A)$ and letting, for all $g \in G$, $[hL, Rk] \in M(G_L, E, {}_RG, P_A)$,

$$g[hL, Rk] = [ghL, Rk], \qquad [hL, Rk]g = [hL, Rkg],$$

and (if $M(G_L, E, {}_RG, P_A)$ has 0)

$$g0 = 0g = 0.$$

It is easy to check that $T(G, L, R, A)$ becomes a regular semigroup.

Let us summarize some properties of the semigroups $T(G, L, R, A)$.

PROPOSITION 1.1. (i) *The identity element of the group G is also the identity of $T(G, L, R, A)$.*

(ii) *$T(G, L, R, A)$ is completely regular if and only if $A = {}_RG_L$.*

(iii) *$T(G, L, R, A)$ is inverse if and only if $A = \{RL\}$.*

(iv) *$T(G, L, R, A)$ is orthodox if and only if it is E-solid and if and only if $A = {}_RH_L$ for some subgroup H of G containing RL.*

(v) *$T(G, L, R, A)$ is noncryptic if and only if $L \neq G$ or $R \neq G$.*

Proof. Statements (i), (ii), and (iii) are obvious. Let us verify (iv).

Suppose first $T(G, L, R, A)$ is E-solid. Let $H = \{g \in G \mid RgL \in A\}$. We are going to check that H is a subgroup of G. Take any $g, h \in H$ and consider the elements $[hL, R]$, $[gL, R]$, and $[gL, Rg^{-1}]$ of $M(G_L, E, {}_RG, P_A)$. Clearly, they are idempotents and $[hL, R]\mathscr{L}[gL, R]\mathscr{R}[gL, Rg^{-1}]$. Then there exists an idempotent f such that $[hL, R]\mathscr{R}f\mathscr{L}[gL, Rg^{-1}]$. However the only element both $\mathscr{R}$-related to $[hL, R]$ and $\mathscr{L}$-related to $[gL, Rg^{-1}]$ is the element $[hL, Rg^{-1}]$ and the fact that it is to be an idempotent implies that $g^{-1}h \in H$. Therefore H is a subgroup and $A = {}_RH_L$.

Now let $A = {}_RH_L$ for a subgroup H of G containing RL. We want to show that $T(G, L, R, A)$ is orthodox, i.e., the product of any two idempotents is an idempotent again. Clearly, we can restrict ourselves to considering idempotents from $M(G_L, E, {}_RG, P_A)$. An element $f = [hL, Rk] \in$

$M(G_L, E, {}_RG, P_A)$ is an idempotent if and only if $RkhL \in A$, so if and only if $kh \in H$. If we take another idempotent, say $d = [qL, Rr] \in M(G_L, E, {}_RG, P_A)$, then $rq \in H$ and either $fd = 0$ (and there is nothing to prove) or $fd = [hL, Rr]$, which case is possible if and only if $kq \in H$. Since H is a subgroup, $kh, kq, rq \in H$ implies that $rh = (rq)(kq)^{-1}(kh)$ belongs to H and therefore $fd = [hL, Rr]$ is an idempotent.

Statement (v) is easy to prove, but we want to verify it, nevertheless, for it plays a crucial role in what follows. Suppose first that $L \neq G$ and take an element $g \in G \setminus L$. Then the elements e and g of the group G are, of course, $\mathscr{H}$-related, whereas the elements $e[L, R] = [L, R]$ and $g[L, R] = [gL, R]$ are not since $L \neq gL$, and multiplying by any element from the right cannot change the left component of the pair $[L, R]$ to gL. Thus $\mathscr{H}$ is not a congruence on $T(G, L, R, A)$. By symmetry, the same it true if $R \neq G$.

Conversely, if $L = G = R$, then $T(G, L, R, A)$ is easily seen to be nothing but G^0 and therefore $\mathscr{H}$ is obviously a congruence on $T(G, L, R, A)$. ∎

The role that the foregoing construction plays in our considerations will be clarified in the next section. Namely, we will show that every noncryptic completely semisimple semigroup has a noncryptic semigroup of the type $T(G, L, R, A)$ as a *regular divisor*, i.e., as a homomorphic image of a regular subsemigroup. Since we are looking for a (in some sense minimal) collection of such regular divisors, we are interested now in studying the relationship between semigroups arising as $T(G, L, R, A)$ when G, L, R, and/or A vary. The first steps here are quite easy and can be done in the most general setting.

LEMMA 1.2. *Let G be a group, L, R be subgroups of G, and A be any subset of ${}_RG_L$ containing RL. If H is a subgroup of G, then the semigroup $T(G, L, R, A)$ contains a subsemigroup isomorphic to $T(H, L \cap H, R \cap H, B)$ where $B = \{(R \cap H)h(L \cap H) | h \in H,\ RhL \in A\}$.*

Proof. Consider the subsemigroup S of $T(G, L, R, A)$ generated by H and the element $[L, R]$. Clearly, it consists of H, all the elements of the kind $[hL, Rk]$, where h, k run over H, and may be 0. It is well known that there are bijections between the cosets of G of the form hL, $h \in H$ (resp. Rk, $k \in H$), and the cosets of H with respect to $H \cap L$ (resp., $H \cap R$). These bijections extend in a obvious way to an isomorphism between S and $T(H, L \cap H, R \cap H, B)$. ∎

COROLLARY 1.3. *Every noncryptic semigroup of the form $T(G, L, R, A)$ contains a noncryptic subsemigroup of the form $T(C, L', R', B)$, where C is a cyclic group.*

Proof. Indeed, if $T(G, L, R, A)$ is noncryptic, then either $L \neq G$ or $R \neq G$ by Proposition 1.1(v). Let, for example, $L \neq G$. Then we can take an element $g \in G \setminus L$ and denote by C the cyclic subgroup it generates. By Lemma 1.2, $T(C, L \cap C, R \cap C, B)$ is isomorphic to a subsemigroup in $T(G, L, R, A)$ and for $L \cap C \neq C$, this subsemigroup is noncryptic. ∎

As Corollary 1.3 shows, we could now restrict ourselves to considering our construction over cyclic groups only. Having in mind some further possible applications, we have preferred, however, to deal with the general situation whenever this creates no unnecessary complications.

LEMMA 1.4. *Let G be a group, L, R be subgroups of G, and A be any subset of ${}_RG_L$ containing RL. Suppose N is a normal subgroup of G such that the set $\{g \in G \mid RgL \in A\}$ is a union of N cosets. Then the natural homomorphism $g \mapsto \bar{g}$ of G onto $\overline{G} = G/N$ extends to a homomorphism of the semigroup $T(G, L, R, A)$ onto the semigroup $T(\overline{G}, \overline{L}, \overline{R}, \overline{A})$, where $\overline{L} = LN/N$, $\overline{R} = RN/N$, and $\overline{A} = \{\overline{R}\bar{g}\overline{L} \mid RgL \in A\}$.*

Proof. Denote the mapping

$$\varphi\colon T(G, L, R, A) \to T\left(\overline{G}, \overline{L}, \overline{R}, \overline{A}\right)$$

by the rules

$$\varphi(g) = \bar{g}, \qquad \varphi([hL, Rk]) = \left[\bar{h}\overline{L}, \overline{R}\bar{k}\right]$$

and (if $T(G, L, R, A)$ has 0)

$$\varphi(0) = 0.$$

Clearly, φ is surjective. To verify that φ is a homomorphism, it suffices to check that $[hL, Rk][qL, Rr] \neq 0$ if and only if $[\bar{h}\overline{L}, \overline{R}\bar{k}][\bar{q}\overline{L}, \overline{R}\bar{r}] \neq 0$ or, in other words, that $RkqL \in A$ if and only if $\overline{R}\bar{k}\bar{q}\overline{L} \in \overline{A}$. The "only if" statement here is a direct consequence of the definition of $\overline{A}$, while the "if" part easily follows from the condition that the set $\{g \in G | RgL \in A\}$ is a union of N cosets. ∎

If both L and R are normal subgroups of a group G, so is their product RL. The condition that the set $\{g \in G | RgL \in A\}$ is a union of RL cosets is automatically satisfied, so Lemma 1.4 applies in this case. We note that we can identify A with $\overline{A}$ in this situation since the set ${}_RG_L$ becomes a group, being nothing but the quotient group G/RL. We obtain the following important corollary.

COROLLARY 1.5. *Let L and R be normal subgroups of a group G. Then for any subset A of G/RL containing RL, the semigroup $T(G/RL, E, E, A)$ is a quotient of the semigroup $T(G, L, R, A)$.*

We use the simplified notation $T(G, A)$ for the semigroup $T(G, E, E, A)$. The set A in this construct becomes merely a subset of G containing e. As it follows from Proposition 1.1(v), $T(G, A)$ is noncryptic whenever G is nontrivial. Therefore Corollary 1.5 implies that we can restrict ourselves to considering semigroups of the form $T(G, A)$ instead of $T(G, L, R, A)$ whenever L, R are normal subgroups—which can be assumed to be always the case in view of Corollary 1.3—and $G \neq RL$.

COROLLARY 1.6. *Let G be a group, L, R be subgroups of G, and N be a normal subgroup of G containing RL. Then the semigroup $T(G/N, E)$ is a quotient of the semigroup $T(G, L, R, {}_RN_L)$.*

Let us proceed now with the case $A = {}_RG_L$. We use the simplified notation $T(G, L, R)$ for the semigroup $T(G, L, R, {}_RG_L)$.

LEMMA 1.7. *Let G be a group and L, R be subgroups of G. Then the semigroup $T(G, L, R)$ is isomorphic to a subdirect product of semigroups $T(G, L, G)$ and $T(G, G, R)$.*

Proof. It is easy to verify that the mappings

$$\lambda\colon T(G, L, R) \to T(G, L, G) \qquad \text{and} \qquad \rho\colon T(G, L, R) \to T(G, G, R),$$

defined by the rules

$$\lambda(g) = \rho(g) = g, \qquad \lambda([hL, Rk]) = [hL, G],$$
$$\rho([hL, Rk]) = ([G, Rk]),$$

are surjective homomorphisms and together they obviously separate the elements of $T(G, L, R)$. ∎

Let us denote by $LT(G)$ (resp., $RT(G)$) the semigroup $T(G, E, G)$ (resp., $T(G, G, E)$).

COROLLARY 1.8. *Let G be a group and L, R be subgroups of G. If the semigroup $T(G, L, R)$ is noncryptic, then it has one of semigroups $LT(\mathbf{C}_p)$ or $RT(\mathbf{C}_p)$ for some prime p as a regular divisor.*

Proof. By Proposition 1.1(v), we may assume that, for example, $L \neq G$. Then the semigroup $T(G, L, G)$, which is a homomorphic image of $T(G, L, R)$ by Lemma 1.7, is also noncryptic. By Corollary 1.3, we may assume that G is a cyclic group. Let N be a maximal proper subgroup of G containing L. Then G/N is isomorphic to $\mathbf{C}_p$ for some prime p and by Lemma 1.4 the natural homomorphism of G onto G/N extends to a homomorphism of $T(G, L, G)$ onto $T(G/N, E, G/N) \cong LT(\mathbf{C}_p)$. ∎

Now we can complete the analysis of semigroups of the form $T(G, A)$.

LEMMA 1.9. *Let G be an abelian group and A be a subset of G containing e. Denote by Z the set of all integers i such that $g^i \neq e$ for some $g \in G$. Then either there exists a nontrivial cyclic group C such that $T(C, E)$ is a Rees quotient of a regular subsemigroup of the direct power $T(G, A)^Z$ or $T(G, A)$ has one of the semigroups $LT(\mathbf{C}_p)$ or $RT(\mathbf{C}_p)$ as a regular divisor.*

Proof. There are two possible cases.

Case 1. *For each $i \in Z$, there exists an element $g_i \in G$ such that $g_i^i \notin A$.* We construct a subsemigroup S in $T(G, A)^Z$ as follows. First, take the element $(\dots, g_i, \dots) \in G^Z$, which we denote by g. Clearly, g generates a nontrivial cyclic subgroup C of G^Z. Further, for every $h = (\dots, h_i, \dots)$, $k = (\dots, k_i, \dots) \in C$ and for every subset $X \subseteq Z$, consider the element

$$\langle h, k, X \rangle = (\dots, a_i, \dots) \in \big(M(G, E, G, P_A)\big)^Z,$$

where $a_i = [h_i, k_i]$ if $i \in X$ and $a_i = 0$ otherwise, and denote by M the set of all such elements. Then let $S = C \cup M$.

It is not hard to verify that S is a subsemigroup. (Indeed, one can check easily that for all $h, k, q, r \in C$, $X, Y \subseteq Z$,

$$q\langle h, k, X \rangle = \langle qh, k, X \rangle, \qquad \langle h, k, X \rangle r = \langle h, kr, X \rangle,$$
$$\langle h, k, X \rangle \langle q, r, Y \rangle = \langle h, r, W \rangle,$$

where W is some subset of $X \cap Y$.) Moreover, S is regular. Clearly, elements of C have inverses and for an element of the form $\langle h, k, X \rangle$, the element $\langle k^{-1}, h^{-1}, X \rangle$ can be straightforwardly verified to be an inverse.

Define a mapping φ: $S \to T(C, E)$ by letting, for all $h, k \in C$, $X \subseteq Z$,

$$\varphi(h) = h, \qquad \varphi(\langle h, k, X \rangle) = \begin{cases} [h, k], & \text{if } X = Z, \\ 0, & \text{otherwise}. \end{cases}$$

Comparing the multiplication rules in S and $T(C, E)$, we see that to verify that φ is a homomorphism, it suffices to show that for all $h, k, q, r \in C$, $\langle h, k, Z \rangle \langle q, r, Z \rangle = \langle h, r, Z \rangle$ in S if and only if $[h, k][q, r] = [h, r]$ in $T(C, E)$. The latter equality is equivalent to the fact that $kq = e$ in C. Since this means that $k_i q_i = e$ for all $i \in Z$, this condition indeed implies $\langle h, k, Z \rangle \langle q, r, Z \rangle = \langle h, r, Z \rangle$. Conversely, suppose that $kq \neq e$. Here we shall finally use our special choice of the element g. Indeed, since kq is an element of the cyclic group generated by g, $kq = g^i$ for some i and this i is to belong to the set Z for $g^i \neq e$. Therefore, by our choice of g, $k_i q_i = g_i^i$ does not belong to A. Now calculating the ith entry of the product $\langle h, k, Z \rangle \langle q, r, Z \rangle$ (i.e., $[h_i, k_i][q_i, r_i]$), we see that the corresponding element of the sandwich matrix P_A equals 0, whence this entry equals 0 too. Thus, $\langle h, k, Z\rangle\langle q, r, Z\rangle \neq \langle h, r, Z\rangle$.

We proved that φ is a homomorphism. Clearly, it is surjective and the corresponding congruence on the semigroup S is nothing other than the Rees congruence with respect to the ideal I of all elements of the form $\langle h, k, X\rangle$, where $X \neq Z$ (i.e., the ideal of all "vectors" from S having a zero entry). Hence the Rees quotient S/I is isomorphic to the semigroup $T(C, E)$.

Case 2. *There exists $i \in Z$ such that, for each $g \in G$, g^i belongs to A.* Let $H = \{g^i | g \in G\}$. Then H is a subgroup of G since G is abelian. In view of our definition of Z, $H \neq E$. Finally $H \subseteq A$ for this case. By Lemma 1.2, $T(G, A)$ has a subsemigroup isomorphic to $T(H, H) = T(H, E, E)$ and Corollary 1.8 applies. ∎

Let us summarize now all the results concerning our construction.

PROPOSITION 1.10. *If a semigroup of the form $T(G, L, R, A)$ is noncryptic, then the e-variety $\mathscr{V}$ it generates contains one of the semigroups $T(\mathbf{C}_\infty, E)$, $T(\mathbf{C}_p, E)$, $LT(\mathbf{C}_p)$, or $RT(\mathbf{C}_p)$ for some prime p.*

Proof. Indeed, if $A =_R G_L$, then Corollary 1.8 applies. Otherwise, Corollaries 1.3 and 1.5 imply that the e-variety $\mathscr{V}$ contains a noncryptic semigroup of the form $T(H, E)$ for some abelian group H. By Lemma 1.9, $\mathscr{V}$ contains either one of the semigroups $LT(\mathbf{C}_p)$ or $RT(\mathbf{C}_p)$ for some prime p or a semigroup of the form $T(C, E)$ for some nontrivial cyclic group C. In the latter case, we can utilize Lemma 1.2 to find one of the semigroups $T(\mathbf{C}_\infty, E)$ or $T(\mathbf{C}_p, E)$ for some prime p in $\mathscr{V}$. ∎

It is easy to see that the semigroups $LT(\mathbf{C}_p)$ and $RT(\mathbf{C}_p)$ are nothing other than Rasin's semigroups $L(p)$ and $R(p)$, respectively, defined in the introduction and the semigroups $T(\mathbf{C}_\infty, E)$ and $T(\mathbf{C}_p, E)$ are isomorphic to Reilly's constructs $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ and $N(\mathbf{C}_p, \mathbf{C}_p)$, respectively. Hence we have

COROLLARY 1.11. *If a semigroup of the form $T(G, L, R, A)$ is noncryptic, then the e-variety it generates contains one of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$, $N(\mathbf{C}_p, \mathbf{C}_p)$, $L(p)$, or $R(p)$ for some prime p.*

The list of minimal "forbidden objects" of Corollary 1.11 cannot be reduced anymore because the e-varieties generated by different semigroups from this list are pairwise incomparable as follows from Theorems 1 and 2.

We finish this section with a result which will be useful in the proof of Theorem 4.

PROPOSITION 1.12. *If a semigroup of the form $T(G, L, R, A)$ is E-solid but is not completely regular, then it contains one of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ or $N(\mathbf{C}_p, \mathbf{C}_p)$ for some prime p among its regular divisors.*

Proof. It follows from Proposition 1.1(ii) and (iv) that if $T(G, L, R, A)$ is E-solid but is not completely regular, then $A = {}_R H_L$ for a proper subgroup H of G containing RL. Take an element $g \in G \setminus H$ and denote by C the cyclic subgroup it generates. By Lemma 1.2, the semigroup $T(G, L, R, A)$ contains a subsemigroup isomorphic to the semigroup $T(C, L', R', B)$, where $L' = L \cap C$, $R' = R \cap C$, and $B = \{R'cL' | c \in C,\ RcL \in A\}$. Let $N = H \cap C$. Then $R'L' \subseteq N \subset C$ and B is easily seen to coincide with ${}_{R'}N_{L'}$. Since C is an abelian group, N is a normal subgroup in C and Corollary 1.6 applies yielding the semigroup $T(C/N, E)$ as a quotient of the semigroup $T(C, L', R', B)$. Now we can again utilize Lemma 1.2 to find in $T(C/N, E)$ a subsemigroup isomorphic to either $T(\mathbf{C}_\infty, E) \cong N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ or, for some prime p, $T(\mathbf{C}_p, E) \cong N(\mathbf{C}_p, \mathbf{C}_p)$. ∎

2. THE PROOF OF THE MAIN RESULT

Let $\mathscr{H}^*$ denote the congruence generated by Green's relation $\mathscr{H}$.

LEMMA 2.1. *Let S be a regular semigroup. Then $\mathscr{H}^*$ is generated by the set of all pairs (a, e), where $e \in E(S)$ and $a\mathscr{H}e$.*

Proof. This follows easily from Green's lemma (see [1, Theorem 2.3]). ∎

LEMMA 2.2. *Let S be a regular semigroup and suppose that $\mathscr{H}$ is not a congruence on S. Then there exists $e \in E(S)$ and $a, b \in S$ such that $a\mathscr{H}e$ and either*

$$be = b \text{ and } ba \text{ are not } \mathscr{L}\text{-related} \tag{1}$$

or

$$eb = b \text{ and } ab \text{ are not } \mathscr{R}\text{-related}. \tag{2}$$

Proof. Take a pair $(c, d) \in \mathscr{H}^* \setminus \mathscr{H}$. By Lemma 2.1, there exists a sequence $c = c_0, c_1, \ldots, c_n = d$ such that, for every $i = 0, 1, \ldots, n-1$, $\{c_i, c_{i+1}\} = \{p_i e_i q_i, p_i a_i q_i\}$, where $p_i, q_i \in S^1$, $e_i \in E(S)$, and $a_i \mathscr{H} e_i$. Since c is not $\mathscr{H}$-related to d, there exists i such that c_i is not $\mathscr{H}$-related to c_{i+1}. Thus we have found $e = e_i$, $a = a_i$, $p = p_i$, and $q = q_i$ such that $e \in E(S)$, $a\mathscr{H}e$, and paq is not $\mathscr{H}$-related to peq. Suppose both $pe\mathscr{L}pa$ and $eq\mathscr{R}aq$. Since $\mathscr{L}$ (resp., $\mathscr{R}$) is known to be a right (resp., left) congruence, this would imply $pe \cdot q\mathscr{L}pa \cdot q$ and $p \cdot eq\mathscr{R}p \cdot aq$, which means $peq\mathscr{H}paq$, a contradiction. Thus either pe and pa are not $\mathscr{L}$-related (and then (1) holds for $b = pe$) or eq and aq are not $\mathscr{R}$-related (and then (2) is true for $b = eq$). ∎

LEMMA 2.3. *Let S be a regular semigroup and suppose that there exists $e \in E(S)$ and $a, b \in S$ such that $a\mathscr{H}e$ and* (2) *holds. Then there exists an idempotent d such that*

$$d \leq e \text{ and } d \text{ is not } \mathscr{R}\text{-related to } ad. \tag{3}$$

Proof. Let b' be any inverse of b and $f = bb'$. It is clear that $ef = f$. Denote fe by d. Then $d^2 = fefe = ffe = fe = d$, $ed = efe = fe = d$, and $de = fee = fe = d$. Thus d is an idempotent and $d \leq e$. Further, $d\mathscr{R}b$. (Indeed, $db = feb = fb = bb'b = b$ and $bb'e = fe = d$.) Since $\mathscr{R}$ is a left congruence, this implies $ad\mathscr{R}ab$. Therefore $d\mathscr{R}ad$ would imply $b\mathscr{R}ab$ which is impossible. Thus d is not $\mathscr{R}$-related to ad. ∎

Recall that a semigroup S is called *completely semisimple* if all its principal factors are completely 0-simple or completely simple. It follows from Andersen's theorem [1, Theorem 2.54] that a regular semigroup is completely semisimple if and only if it has no bicyclic subsemigroups. Thus, the following statement from [9] allows us to restrict ourselves to considering completely semisimple semigroups only.

LEMMA 2.4 (Reilly [9, Theorem 5.12]). *The semigroup $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ belongs to the e-variety generated by the bicyclic semigroup and thus to any e-variety of regular semigroups containing a semigroup that is not completely semisimple.*

PROPOSITION 2.5. *Let a completely semisimple semigroup S contain an element a and idempotents e, d such that $a\mathscr{H}e$ and* (3) *holds. Then S has a noncryptic semigroup of the form $T(G, L, R, A)$ for some cyclic group G among its regular divisors. If the element ad does not belong to* $\operatorname{Gr} S$, *then we can in addition assume that $A \neq_R G_L$.*

Proof. Denote by G the subgroup of S generated by a and by H the subgroup of the $\mathscr{H}$-class containing d, which is generated by all the elements dgd, $g \in G$, such that $dgd\mathscr{H}d$. Let us consider also the ideal $I = J(d) \setminus J_d$ of S (I might be empty, which affects no step in the reasoning below). Since S is supposed to be completely semisimple, the principal factor $J(d)/I$ is completely [0]-simple, which easily implies that, for any $g \in G$, the element dgd belongs to either H or I. We denote by T the subsemigroup of S generated by G, H, and I. It is easy to see that T is a regular semigroup.

Let M denote the $\mathscr{J}$-class of d in T. Then a typical element $t \in M$ may be written in the form

$$t = hd(dg_1d)^{\varepsilon_1}(dg_2d)^{\varepsilon_2} \cdots (dg_nd)^{\varepsilon_n} dk,$$

where $h, k, g_1, \dots, g_n \in G$, $dg_1d, \dots, dg_nd \in H$, and $\varepsilon_1, \dots, \varepsilon_n \in \{1, -1\}$. It is clear that $hd\mathscr{R}t\mathscr{L}dk$.

Consider the sets $L = \{g \in G | gd\mathscr{R}d\}$ and $R = \{g \in G | dg\mathscr{L}d\}$, which can be easily verified to be subgroups of G. We note that $L \neq G$ for $a \notin L$ in view of (3). Clearly, the left cosets with respect to L are in a one-to-one correspondence with the $\mathscr{R}$-classes of M, whereas the right cosets with respect to R index its $\mathscr{L}$-classes. Consider now the relation γ on T that coincides with the identity relation on G, with Green's relation $\mathscr{H}$ on M, and with the universal relation on I. It can be checked straightforwardly that γ is a congruence on T. Furthermore, the elements of M/γ are in a one-to-one correspondence with the pairs of the form $[hL, Rk]$, where hL runs over G_L and Rk runs over ${}_RG$. If we denote by A the set of all double cosets $RgL \in {}_RG_L$ such that $dgd\mathscr{H}d$, then we see that the product $[hL, Rk] \cdot [qL, Rr]$ belongs to M/γ (and then equals to $[hL, Rr]$) if and only if $RkqL$ is in A. Thus, T/γ is isomorphic to $T(G, L, R, A)$ (or may be to $T(G, L, R, A)$ with 0 adjoined if the ideal I is nonempty while $A = {}_RG_L$). Proposition 1.1(v) then implies that $T(G, L, R, A)$ is noncryptic because $L \neq G$.

Suppose finally that the element ad does not belong to $\operatorname{Gr} S$. Then, in particular, the $\mathscr{H}$-class of this element is not a subgroup. Since the principal factor $J(d)/I$ is completely [0]-simple, this implies that $(da)^2 = dada \in I$ and therefore $dad = dada \cdot a^{-1} \in I$. Thus $dad \notin H$ which, in view of the definition of the set A, means that $RaL \notin A$. ∎

Now we are able to complete the proof of the main theorem. Suppose that $\mathscr{V}$ is a noncryptic e-variety. If it contains a semigroup that is not completely semisimple, then by Lemma 2.4, the semigroup $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ belongs to $\mathscr{V}$. Otherwise it contains a completely semisimple noncryptic semigroup S. Lemmas 2.2 and 2.3 show that we may assume that the conditions of Proposition 2.5 are satisfied, so that a noncryptic semigroup of the form $T(G, L, R, A)$ is a regular divisor of S. Therefore $\mathscr{V}$ contains this noncryptic semigroup $T(G, L, R, A)$.

Corollary 1.11 then shows that the e-variety $\mathscr{V}$ contains one of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$, $N(\mathbf{C}_p, \mathbf{C}_p)$, $L(p)$, or $R(p)$ for some prime p. By Theorems 1 and 2 each of these semigroups generates a minimal noncryptic e-variety and therefore Theorem 3 follows. ∎

3. COROLLARIES AND APPLICATIONS

Let us start with some corollaries that immediately follow from Theorem 3. The first of them generalises the result by Doyle mentioned in the Introduction.

COROLLARY 3.1. *An e-variety of regular semigroups is cryptic if and only if its intersections with the variety of all completely regular semigroups and the variety of all inverse semigroups are cryptic.*

Proof. Necessity is clear. Sufficiency follows from Theorem 3 since all minimal noncryptic e-varieties are either inverse or completely regular. ∎

In [10, Theorem 3.6], an equational characterization of cryptic e-varieties of E-solid semigroups has been found. Namely, it was proved that an e-variety $\mathscr{V}$ of E-solid semigroups is cryptic if and only if there exists a positive integer n such that every semigroup $S \in \mathscr{V}$ satisfies the condition

$$(x^n, x^{n+1}) \in \mu, \tag{4}$$

where μ stands for the maximum idempotent-separating congruence on S. (See [10, Remark 3.5] for an explanation of how the latter condition can be expressed in terms of identities on an arbitrary regular semigroup.) Our next corollary shows that this equational characterization remains valid in the class of all group-bound e-varieties of regular semigroups. (Recall that an e-variety $\mathscr{V}$ is called *group-bound* if there exists a positive integer n such that in every semigroup $S \in \mathscr{V}$ the nth power of each element belongs to $\operatorname{Gr} S$.)

COROLLARY 3.2. *A group-bound e-variety $\mathscr{V}$ of regular semigroups is cryptic if and only if it satisfies* (4) *for some positive integer n.*

Proof. Necessity. If a regular semigroup S is cryptic, then $\mu = \mathscr{H}$ and therefore $(x^n, x^{n+1}) \in \mu$ whenever x^n belongs to a subgroup of S.

Sufficiency. It is easy to verify that the maximum idempotent-separating congruence on each of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$, $N(\mathbf{C}_p, \mathbf{C}_p)$, $L(p)$, or $R(p)$ is trivial and therefore none of them satisfies (4) for any n. Now Theorem 3 applies. ∎

Since every cryptic e-variety is completely semisimple (by Lemma 2.4) and completely semisimple E-solid e-varieties are exactly group-bound E-solid e-varieties ([10, Theorem 2.11]), Corollary 3.2 indeed generalises the result by Yeh mentioned before its formulation. We note also that if each completely semisimple e-variety of regular semigroups is group-bound (which is unknown so far), then the argument of Corollary 3.2 would give an equational description of cryptic e-varieties in the class of all e-varieties of regular semigroups.

Now we are going to prove Theorem 4. We shall make use of a well known characterization of E-solid e-varieties due to Hall.

LEMMA 3.3 (Hall [4, Corollary 3.6]). *An e-variety of regular semigroups is E-solid if and only if it does not contain C_2.*

It is well known that in an E-solid semigroup S the product of any two idempotents belongs to $\operatorname{Gr} S$. For an element $a \in \operatorname{Gr} S$, we denote by a^0 the identity element of the maximal subgroup containing a.

LEMMA 3.4. *Let S be an E-solid semigroup and a, b be elements from $\operatorname{Gr} S$. If ab does not belong to $\operatorname{Gr} S$, then either ab^0 or a^0b does not belong to $\operatorname{Gr} S$.*

Proof. Clearly, $ab^0 \mathscr{L} a^0b^0 \mathscr{R} a^0b$. Suppose $ab^0, a^0b \in \operatorname{Gr} S$. Then since $a^0b^0 \in \operatorname{Gr} S$ as well, we can substitute the corresponding idempotents for all these three elements getting $(ab^0)^0 \mathscr{L} (a^0b^0)^0 \mathscr{R} (a^0b)^0$. Since S is E-solid, there exists an idempotent, say e, such that $(ab^0)^0 \mathscr{R} e \mathscr{L} (a^0b)^0$ and hence $ab^0 \mathscr{R} e \mathscr{L} a^0b$. On the other hand, $ab^0 \mathscr{R} ab \mathscr{L} a^0b$. Combining these two observations, we get $ab \mathscr{H} e$ and therefore $ab \in \operatorname{Gr} S$, a contradiction. ∎

LEMMA 3.5. *Let S be an E-solid semigroup, a be an element from $\operatorname{Gr} S$, and f be an idempotent. If af does not belong to $\operatorname{Gr} S$, then there exists an idempotent d such that $d \le a^0$ and ad does not belong to $\operatorname{Gr} S$.*

Proof. Let $d = (a^0f)^0a^0$. Then d is easily seen to be an idempotent, $d \le a^0$, and $df = (a^0f)^0a^0f = (a^0f)^0$. This immediately implies that $ad \mathscr{L} d \mathscr{R} (a^0f)^0$. If $ad \in \operatorname{Gr} S$, then we would have also $(ad)^0 \mathscr{L} d \mathscr{R} (a^0f)^0$. Since S is E-solid, there exists an idempotent, say e, such that $(ad)^0 \mathscr{R} e \mathscr{L} (a^0b)^0$ and hence $ad \mathscr{R} e \mathscr{L} (a^0f)^0$. On the other hand, $ad \mathscr{R} a(a^0f)^0 \mathscr{L} (a^0f)^0$. Combining these two observations, we get $a(a^0f)^0 \mathscr{H} e$ and therefore $a(a^0f)^0 \in \operatorname{Gr} S$. Now Lemma 3.4 applies (with the element a^0f in the role of b) and we obtain that $a \cdot a^0f = af$ belongs to $\operatorname{Gr} S$, a contradiction. ∎

We are ready to complete the proof of Theorem 4. First of all, it is easy to verify that none of the semigroups C_2, $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$, or $N(\mathbf{C}_p, \mathbf{C}_p)$ is group-closed whence the e-varieties they generate are non-group-closed as well. Now let $\mathscr{V}$ be any non-group-closed e-variety of regular semigroups. We are going to prove that it contains one of the semigroups C_2, $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$, or $N(\mathbf{C}_p, \mathbf{C}_p)$ for some prime p.

If $\mathscr{V}$ is not E-solid, then it contains C_2 in view of Lemma 3.3. If $\mathscr{V}$ contains a semigroup that is not completely semisimple, then Lemma 2.4 applies showing that $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ belongs to $\mathscr{V}$. Thus, we may suppose that

$\mathscr{V}$ contains a completely semisimple E-solid non-group-closed semigroup S. Lemmas 3.4 and 3.5 then show that S may be assumed to have an element $a \in \operatorname{Gr} S$ and an idempotent d such that $d \leq e = a^0$ and $ad \notin \operatorname{Gr} S$. The latter property implies, in particular, that elements d and ad cannot be $\mathscr{R}$-related. Since $a\mathscr{H}e$, we see that we are in the condition of Proposition 2.5, which yields a semigroup of the form $T(G, L, R, A)$ with $A \neq_R G_L$ as a regular divisor of S. Since this semigroup is E-solid but is not completely regular, we are in the position to apply Proposition 1.12, which says that one of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ or $N(\mathbf{C}_p, \mathbf{C}_p)$ for some prime p is a regular divisor of $T(G, L, R, A)$ and so belongs to $\mathscr{V}$.

It remains to prove that the e-varieties generated by one of the semigroups C_2, $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$, or $N(\mathbf{C}_p, \mathbf{C}_p)$ are pairwise incomparable. In view of Theorem 2 we need only to verify that the e-variety $\mathscr{C}$ generated by C_2 is incomparable with each of e-varieties generated by one of the semigroups $N(\mathbf{C}_\infty, \mathbf{C}_\infty)$ or $N(\mathbf{C}_p, \mathbf{C}_p)$, but this is clear for $\mathscr{C}$ contains no nontrivial groups but fails to be inverse. Theorem 4 is proved.

As an immediate corollary of Theorems 3 and 4 we get, for example, the following characterization of E-solid cryptic e-varieties:

COROLLARY 3.6. *An E-solid e-variety $\mathscr{V}$ is cryptic if and only if for each $S \in \mathscr{V}$, $\operatorname{Gr} S$ is a band of groups.*

We have to mention that for the orthodox case an analogous result was already known; compare [2, Lemma 2.14].

For the inverse case, both the properties "being cryptic" and "being group-closed" turn out to be equivalent as follows from Theorems 2 and 4. Strangely enough, this observation seems not to have been formulated yet in an explicit form.

COROLLARY 3.7. *An inverse semigroup variety is cryptic if and only if it is group-closed.*

ACKNOWLEDGMENTS

This work was started when the second author was visiting Marquette University and was continued while the first author visited Ural State University. Thus the authors wish to express their gratitude to both these organizations for the perfect working conditions during their visits. The authors are also indebted to Dr. P. G. Trotter, Dr. K. Auinger, and Dr. P. R. Jones for many useful discussions.

REFERENCES

1. A. H. Clifford and G. B. Preston, "The Algebraic Theory of Semigroups. I," Am. Math. Soc., Providence, 1961.

2. J. Doyle, On existence varieties of orthodox semigroups, *J. Austral. Math. Soc. Ser. A*, to appear.
3. T. E. Hall, Identities for existence varieties of regular semigroups, *Bull. Austral. Math. Soc.* **40** (1989), 59–77.
4. T. E. Hall, Regular semigroups: amalgamation and the lattices of existence varieties, *Algebra Universalis* **28** (1991), 79–102.
5. T. E. Hall and P. R. Jones, On the lattice of varieties of bands of groups, *Pacific J. Math.* **191** (1980), 327–337.
6. J. Kaďourek and M. B. Szendrei, A new approach in the theory of orthodox semigroups, *Semigroup Forum* **40** (1990), 257–296.
7. V. V. Rasin, On the varieties of Cliffordian semigroups, *Semigroup Forum* **23** (1981), 201–220.
8. N. R. Reilly, Varieties of completely semisimple inverse semigroups, *J. Algebra* **65** (1980), 427–444.
9. N. R. Reilly, Minimal non-cryptic varieties of inverse semigroups, *Quart. J. Math. Oxford Ser.* (2) **36** (1985), 467–487.
10. Y. T. Yeh, On existence varieties of E-solid or locally inverse semigroups and e-invariant congruences, *J. Algebra* **164** (1994), 500–514.